Security in Management's Terms

By translating audit findings about technology weaknesses into actions CEOs can take, auditors can make IT governance a top business priority.

BY JACKIE BASSETT

INFORMATION SECURITY BREACHES can have a disastrous effect on an organization's day-to-day operations. Besides pointing to ineffective information security controls, policies, and procedures, a breach may signal an absence of sound information technology (IT) governance. IT governance is a component of corporate governance that applies a disciplined process to the availability, usability, integrity, and security of the data relied on by an enterprise. The true value of an information security audit goes beyond compliance. An effective audit can enhance the organization's security stance, further its mission, and act as a catalyst that promotes sound IT governance.

Unfortunately, the technical nature of information security audits makes it difficult for auditors to convey recommendations to senior management adequately. However, with a little preparation and knowledge, auditors can enhance the way they communicate information security audit results and provide recommendations senior executives can implement.

SECURITY'S BUSINESS IMPACT

To ensure information security audit reports are read and understood, internal auditors must provide more than a simple checklist of audit recommendations. They need to translate security recommendations into information chief executive officers (CEOs) and other senior managers will find useful. CEOs, who speak in terms of gross margins and earnings, may not have the technology knowledge needed to translate recommendations into a plan of action that aligns with enterprisewide initiatives or understand how information security controls can help the organization's bottom line and contribute to regulatory compliance. Audit recommendations that refer back to enterprisewide strategic goals and objectives will be more readily adopted. When they don't, information security recommendations get lost in translation, and IT governance efforts take a back seat on management's agenda.

The goal of IT governance is to ensure that the organization's information systems deliver on business performance objectives. It provides business assurance that the data that executives rely on to make business strategy decisions is being captured, processed, and delivered through IT systems accurately. Although auditing for security weaknesses is a critical component of an IT audit, auditing for business assurance is equally important.

Internal auditors' knowledge of security and other IT compliance best practices can help them promote the significance of IT governance. Questions pertaining to IT governance that auditors should keep in mind include:

- What is the business value of IT governance, and how can information security audit recommendations add value?
- How can information security strategies contribute to increased revenues, profitability, and shareholder value?
- What is the relevance and perceived value of information security audit recommendations to the organization's CEO and other senior executives?

While addressing these questions, auditors should present the findings in a way that enables CEOs to take action and helps make IT governance a top business priority. Take for example an information security audit report from a public company indicating that some of the organization's quality assurance (QA) reporting systems had critical interoperability failures. Necessary application controls were missing, posing a serious security risk to the company's customer

service activities. These missing controls were the result of faulty programming code during the software development phase. In this scenario, how do audit recommendations translate into CEO items for immediate action?

Auditors could answer this question by indicating how the implementation of effective IT controls and monitoring mechanisms could enable companies to have the QA controls needed to identify programming errors earlier in the product's life cycle. This could result in a higher quality application that helps the company bring in expected sales revenues. In addition, sound QA controls could help internal auditors bring IT governance best practices to the forefront and allow the CEO to understand how effective IT controls benefit the company's profit margin and stock price.

At the same time, auditors could point out the negative consequences of not implementing audit recommendations. Disregarding recommendations to fix QA control deficiencies could lead to a security breach that compromises the integrity of sensitive customer information.

CLOSING COMMUNICATION GAPS

Raising awareness of IT governance and security controls requires effective communication with executives throughout the audit process. Auditors must take steps before, during, and after an audit to enhance how they report their findings.

BEFORE THE AUDIT In preparation for an information security audit, auditors should meet with senior executives to lay a foundation of trust and teamwork. At this meeting, auditors need to ask executives what their key business goals are and incorporate that information into the audit plan. Action items should map to existing enterprisewide goals to better promote IT governance.

Making the effort to gain a better understanding of the business and what matters most to executives will demonstrate the auditor's commitment to the organization's mission and goals. It will also enable auditors to request a reciprocal investment of time and energy from senior executives, especially when requesting that they assign specific staff to support the audit process.

DURING THE AUDIT Communication should become an integral part of the audit process. If requests are not being fulfilled, auditors should make every effort to request the information that is relevant to the audit plan. This includes information that maps directly to the data senior executives use to make informed decisions about the enterprise's goals. Having this necessary information helps to maximize the audit's results.

One situation where effective communication can maximize audit results is during a live-incident response. For example, many internal auditors have detected an active security exploit during the course of an information security review. If the audit team is not careful, any misstep could modify or destroy evidence of the exploit and affect its admissibility in court. Clear communication between the incident response team and the audit team will limit potential damage and enhance the organization's chances of catching the perpetrator.

Communicating the preliminary results of the audit should begin as soon as a measurable gap has been detected


© 2006 KPMG LLP, the U.S. member firm of KPMG International, a Swiss cooperative.
Enterprise risk management requires the right focus.
And an adviser with vision.
Whether you see it or not, enterprise risk is out there. And its consequences can threaten your business strategy, your brand, even your corporate existence. That's where KPMG's Enterprise Risk Management services can help. We'll work with you to establish an ongoing program to help identify, assess and manage risk. So you have the risk insight you need to improve your business, protect your stakeholders and achieve your strategic vision. For more information contact John M. Farrell, Partner, at 212-872-3047.
www.us.kpmg.com
AUDIT ▪ TAX ▪ ADVISORY
KPMG

between the expected results of the audit and the actual results. Auditors should not wait until the end of the audit to discuss their recommendations. Instead, they should meet regularly with the IT staff assigned to support the audit, restate the goals behind the review, and ask for accountability from senior executives. These meetings should focus on the report's preliminary conclusions, initial recommendations for changes in the security strategy, and the best way to present the audit report to the audit committee. Frequent communication can ensure that auditors, IT staff, and senior executives agree on the right expectations by the time the draft is ready as well as increase the probability that report recommendations are read and implemented.

AFTER THE AUDIT Reports that conclude with "controls should be strengthened" are not actionable and don't help to enhance the organization's information security and IT governance posture. Therefore, recommendations need to provide sufficient information that can be turned into specific action items for implementation, such as recommending the use of intrusion detection, access rights, and other logical access controls to restrict access to files on individual computers and the network. To provide executives with report recommendations that meet strategic corporate objectives, action items need to satisfy information security control objectives, help improve business agility, and strengthen security.

When presenting the report's recommendations to senior executives, auditors can use the meeting as an opportunity to discuss alternative options for existing information security controls. Auditors also can help interpret and explain the business value behind security control objectives. Without a clear and consistent understanding of these objectives, senior executives may implement an information security control that does not meet internal and external security compliance requirements.

A CLEAR ACTION PLAN

For CEOs to give IT governance the attention it deserves, the language and focus of audit reports need to change, especially in the realm of information security. For audit results to be implemented, and IT governance to become a priority, information security audit reports need to provide an action plan in clear business language. Internal auditors who proactively reach out to senior management throughout the entire audit process set the stage for audit success and help to better promote the implementation of security recommendations and effective IT governance.

JACKIE BASSETT is chief executive officer at BT Industrials Inc., a management and technology consulting company based in Washington, D.C.

To comment on this article, e-mail the author at jackie.bassett@theiia.org.

Send "Tech Forum" story ideas to:
Tim McCollum
The Institute of Internal Auditors Inc.
247 Maitland Ave.
Altamonte Springs, FL 32701 USA
e-mail: tim.mccollum@theiia.org